EXHIBIT 38

massport **memo**

CONFIDENTIAL

TO: Virginia Buckingham
FROM: Joseph M. Lawless

DATE: April 27, 2001

SUBJECT: Airport vulnerabilities

Airports have historically been targets of terrorism. The federal government has categorized airports as, "critical infrastructures", vital to our national security interests. There are no specific threats to Logan Airport., however, several incidents occurring over the last few years indicate existing vulnerabilities. The lack of a significant negative consequence, or the loss of a life, does not diminish the seriousness of the vulnerabilities. There was one ingredient missing from those incidents that defined them as a minor security problem instead a catastrophic terrorist event. That ingredient was malicious intent. The effect of those incidents would have been drastically different if the perpetrators had malicious intent.

Unfortunately, a paradigm shift is occurring within the world of terrorism. Federal security and intelligence agencies are predicting an increase in the likelihood of a terrorist attack occurring on U.S. soil in the next few years. The federal government was successful in disrupting potential terrorist events planned for Millennium celebrations. Terrorist organizations have support groups throughout the world. These groups, otherwise known as cells, conduct fundraising, intelligence gathering, recruitment and occasional tactical operations. [redacted]

Intelligence on specific groups is difficult to obtain. The intelligence gathering agencies are not open to sharing information that is difficult to compile. Specific threat information is even more elusive for the end users. In the case of actual terrorist events that have occurred within the U.S., i.e. World Trade Center and Oklahoma City bombings, specific threat information was not available.

The best defense is a good offense. A good offense in the security arena is to harden the potential target. Identifying and eliminating vulnerabilities is the methodology employed to harden the target. Through a series of vulnerability assessments conducted by the FAA, FBI, US Postal Service, and consultants contracted by Massport, vulnerabilities have been identified. Many of the vulnerabilities have been addressed through capital improvements and operational adjustments. We are currently in the early stages of a security assessment of all of our facilities. Notwithstanding that assessment, there are existing vulnerabilities that must be addressed.

AIR OPERATIONS AREA (AOA)

Perimeter Security - The existing perimeter is controlled by a variety of barriers. Those barriers include Chain Link Fence topped with barbed wire, solid concrete blast wall topped w/barbed wire, staffed access gates, automatic key card gates, gates with lock and key control, buildings, and Boston Harbor. The aviation fuel supply is located within the AOA perimeter. The variety of perimeter control barriers and the lack of perimeter controls in other areas make it extremely difficult, if not impossible to defend. The previously mentioned security incidents that could have resulted in catastrophic disasters were breeches in the AOA perimeter. A fourteen (14) year old climbed the security fence in the North cargo area of the airport and in broad daylight, traversed the AOA for one half mile, undetected. The youth unscreened, illegally boarded a British Airways 747, and flew to London. The youth could have easily introduced an explosive device or weapon onto that aircraft. The second incident involved a breech of the AOA

MP100700

RECYCLED PAPER

perimeter at the fuel farm. An unauthorized male was observed climbing down the exterior stairs of a fuel tank late one night. The intruder was able to scale the perimeter fence and climb to the top of the fuel tank, undetected. An observant fuel farm worker spotted the intruder, attempting to exit the area. The intruder could have easily introduced an explosive device into the fuel farm area. The results would have been devastating to the airport and the surrounding East Boston neighborhood. There have been numerous instances of clam diggers, fishermen, hunters and boatsmen entering the AOA from the waterside. An intrusion detection system combined with CCTV and a reengineered perimeter line would greatly enhance today's security.

Access Control – When the access control system was installed more than ten years ago, a decision was made to allow tenants to control access to the AOA, through their controlled space. That decision has resulted in an inconsistent and sometimes ineffective control of access to the AOA. Security controls vary from air carrier to air carrier. The different types of controls used by the carriers include lock and key, cypher lock, scramble locks, and alarms. These alarms are supposed to be monitored by the carriers. Indications are the carriers are not performing these security functions. On numerous occasions, these doors can be compromised because the alarms have been bypassed, or, no one responds to the alarm. Piggybacking through tenant and airport controlled security doors is a recurring problem. There is no way to recreate or investigate a breech of security through these doors under existing conditions. Emergency doors, rooftop hatches, crawl spaces and utility tunnels are additional areas that require access controls. Massport installed access control equipment, anti-piggybacking technology and CCTV are the most likely solutions to these problems.

Anti-terrorism – It is difficult to predict when, where and how a terrorist attack will occur. We have considered the most common weapons and tactics terrorists are using today and have begun programs to meet the threat. Car and vehicle bombs are weapons that have been used around the world and within the U.S. The intermodal nature of an airport requires passengers arrive and depart in some manner, usually an automobile. The extensive curb frontage requires constant attention to unattended vehicles. An explosive damage engineering study has provided insight to vulnerable areas within the airport. An integrated CCTV, motion detection and notification system, would enhance the protection from vehicles left unattended at the curbs. A Weapons of Mass Destruction training and response program are under way. Firefighters and State Police are being trained to recognize chemical and biological agents which have been used by terrorists. Special response equipment is being purchased to assist in the detection and the public safety response to such an incident. Trash receptacles throughout the airport are good hiding places for explosive devices. A bomb proof trash receptacle has been tested within the airport and a trash receptacle replacement program is planned for this budget season.

Identification and control – The airport is responsible to granting AOA unescorted access privileges to employees. Air carriers and tenants must certify that employees have received training in airport security before a security identification card is issued. The level and quality of training vary among the carriers and tenants. Many airports train all employees. Massport has developed a supervisor security training program, but we should consider training all airport employees. Electronic fingerprinting and an expanded list of disqualifying crimes has improved the level of character of employees receiving unescorted access privileges. Additional record checks by the State Police have shown some deficiencies in the electronic fingerprinting program. The electronic fingerprinting program allows for compliance with FAA rules and a faster turnaround on badge production. The additional State Police record checks will continue. Employees of the airport can come and go freely after they have received their unescorted access privileges. Vendors are allowed to be escorted onto to the AOA without being screened. Limiting employees to certain entrances and screening all employees and vendors through metal detectors and x-rays would enhance the overall security of the airport. Other airports do screen all employees entering the AOA. There is no requirement to do this.

Screening of passengers and baggage -- The performance of screeners at the security checkpoints is inconsistent. Recent covert efforts to sneak contraband beyond security by a local news media outlet have shown extremely poor job performance by the security checkpoint operators. There are four companies operating screening checkpoints at the airport. All four companies allowed the media personnel to sneak items through the checkpoints. This is an air carrier responsibility. The screening companies job

performance damages the entire security environment at the airport. The FAA has spent hundreds of millions of dollars in new Explosive Detection Systems (EDS). The EDS are the only approved systems able to detect explosive materials in checked bags. Logan only has one of these machines. It is deployed at U.S. Airways. The equipment is distributed through the FAA's Security Equipment Integrated Product Team, (SEIPT). The SEIPT is dominated by FAA and air carrier personnel. There are three airport delegates on the SEIPT. I am one of the airport delegates on the SEIPT. As a result of my involvement, we will begin to see more of the high tech security screening equipment coming to Logan.

E-911 – Massport is not currently a primary answering point for E-911. All 911 calls for emergencies originating at the airport get routed and answered at Boston Police Headquarters. The calls or information about the calls then get forwarded to the airport. There are safety and security implications of not being a primary answering point. There have been several occasions where Massport has not received notification of emergencies. The lack of notification detracts from our ability to deliver our high level of emergency services. It also inhibits our ability to timely follow up on incidents such as threatening calls. Massport should have its own E-911primary answering point. The E-911 system could be tied in with the state of the art CCTV system that would enable the emergency operator to view the public telephones where the calls were originating.

Workplace violence – Massport has a good policy and training on workplace violence. We have assessed some physical and operational improvements in preventing and responding to workplace violence. The installation of panic hardware will improve response times to potential workplace violence incidents. A CCTV interface with the panic alarm system would also benefit the response and may act as a deterrent to a potential incident. Employees and visitors will be required to display Massport issued identification badges.

This memorandum has outlined Massport's most serious vulnerabilities at this time. I would like a meeting with you at your earliest convenience to discuss solutions I have developed to deal with these vulnerabilities.